Virtual Private Networks (VPNs)
Simplified

Erich Spengler

CSSIA CATC—Moraine Valley Community College
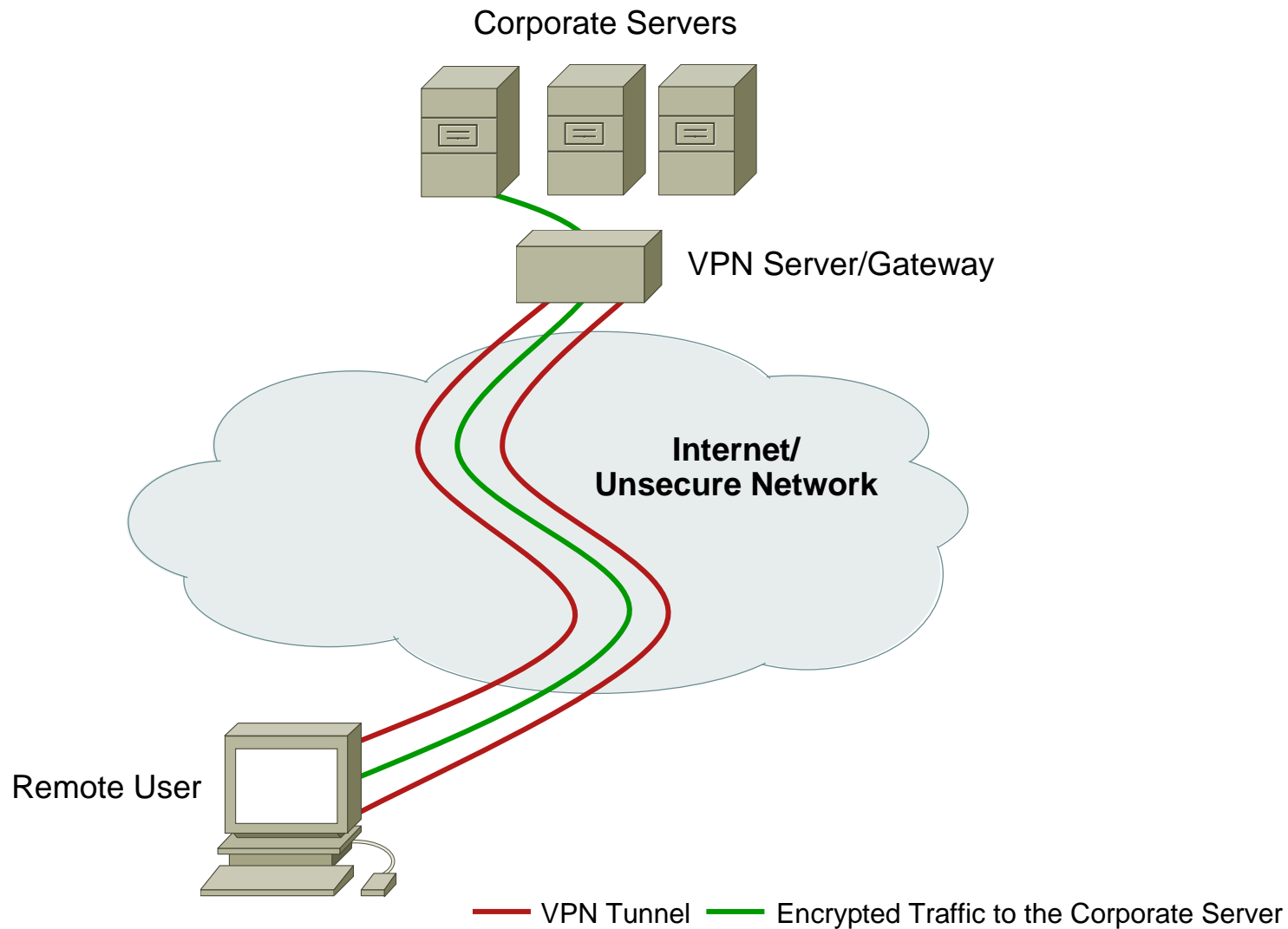
2008—60 Minute Session

Cisco | Networking Academy®
Mind Wide Open™

Cisco Public

Agenda

- Demonstration

- Introduction to VPNs

- VPN Security (IPSec, PPTP, SSL)

- VPN Technology Comparison

- VPN Group Exercise

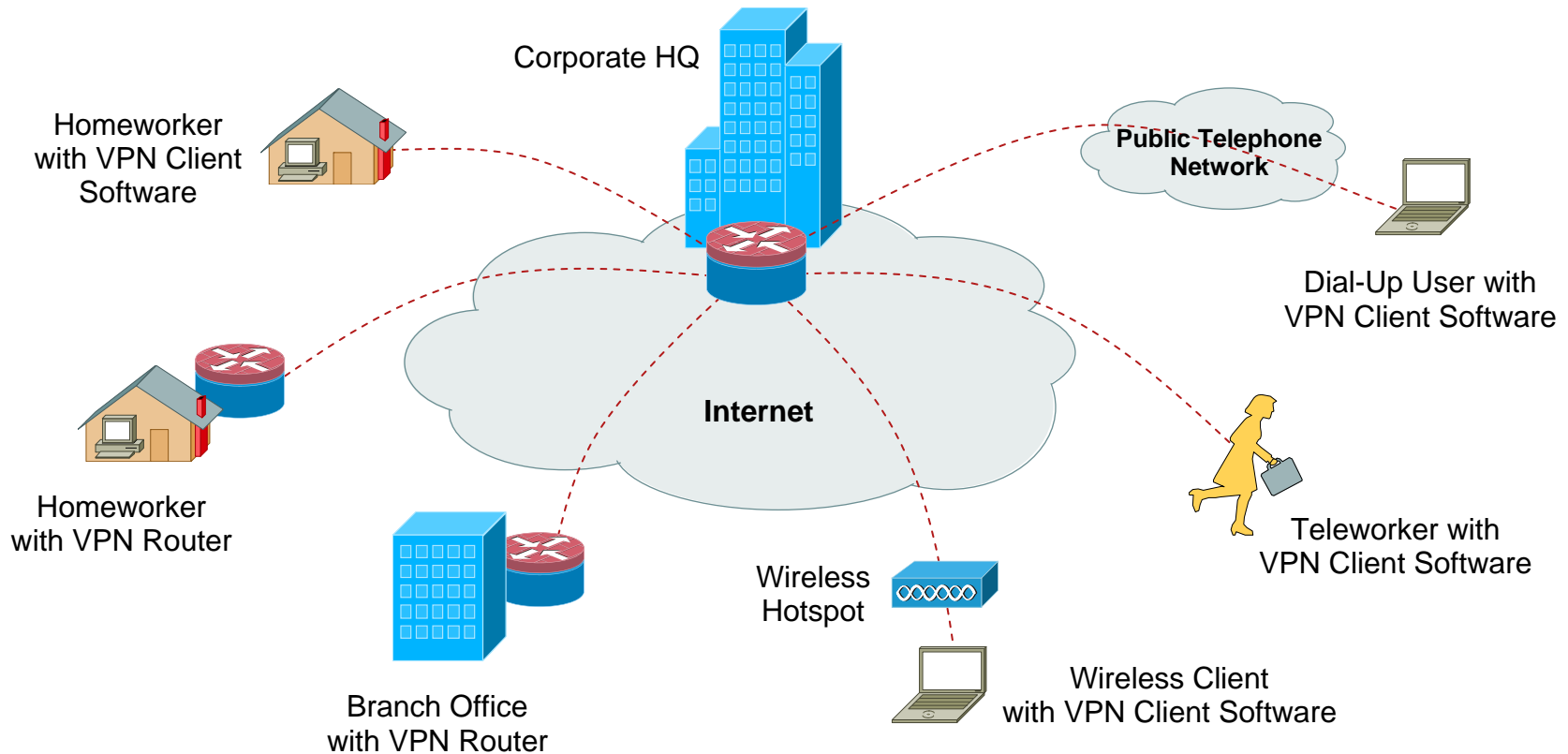# Demonstration—Remote Network Access via VPN

Corporate Servers

VPN Server/Gateway

Internet/ Unsecure Network

Remote User

—— VPN Tunnel —— Encrypted Traffic to the Corporate Server

Cisco Public
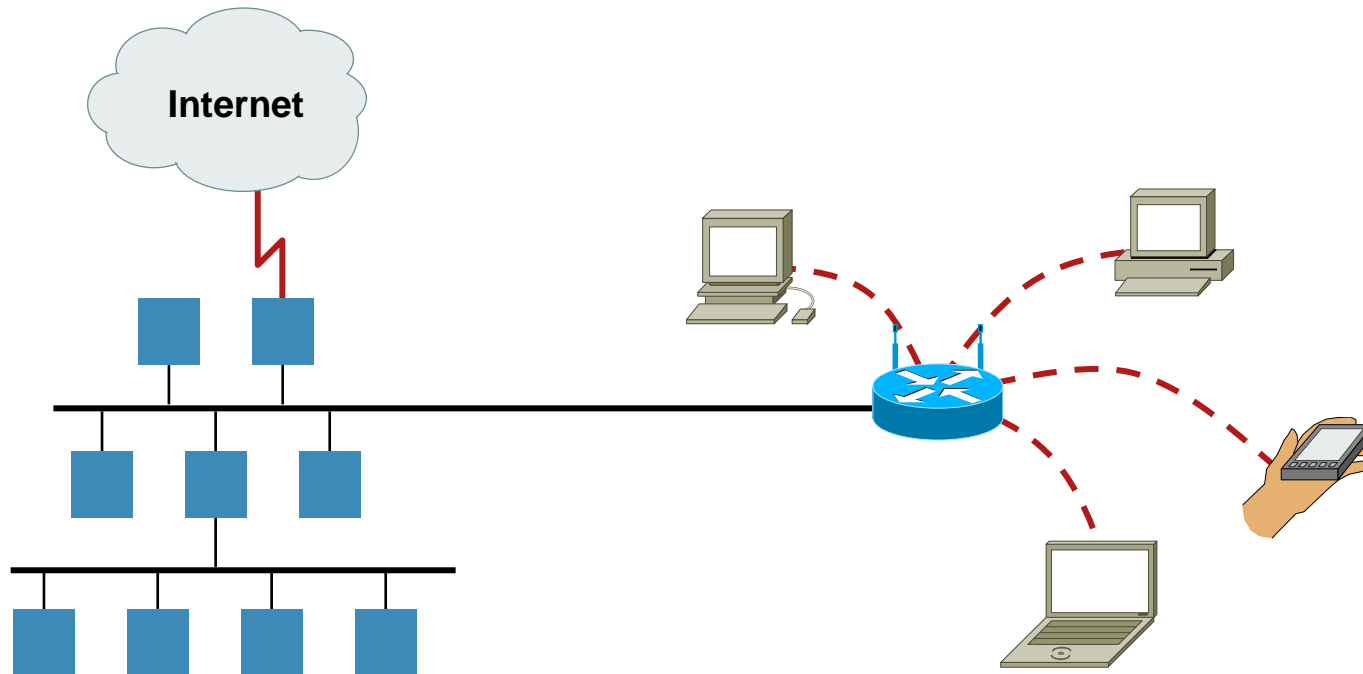
Introduction to VPNs

Cisco Public

What Is a Virtual Private Network (VPN)?

A Remote Access VPN secures connections for remote users, such as mobile users or telecommuters, to corporate LANs over shared service provider networks

Wireless: A New Big Driver for VPNs

- An access point (AP) is a shared device
- Remember the performance issues of shared hubs
- Bridges, and other devices allow for interconnection
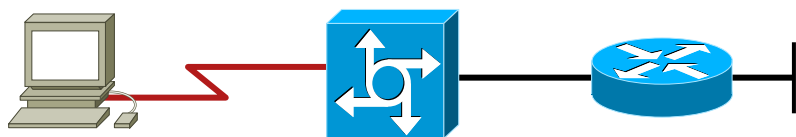- Protocols and applications work seamlessly
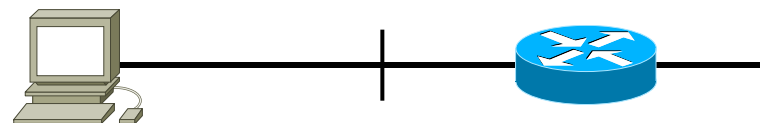
Basic VPN Terms

Router to Router VPN Gateway
(Extranet)

Router to VPN Firewall Gateway
(Extranet)

VPN Client to Router VPN via Dial-Up
(Access VPN)

VPN Client to Router VPN Network
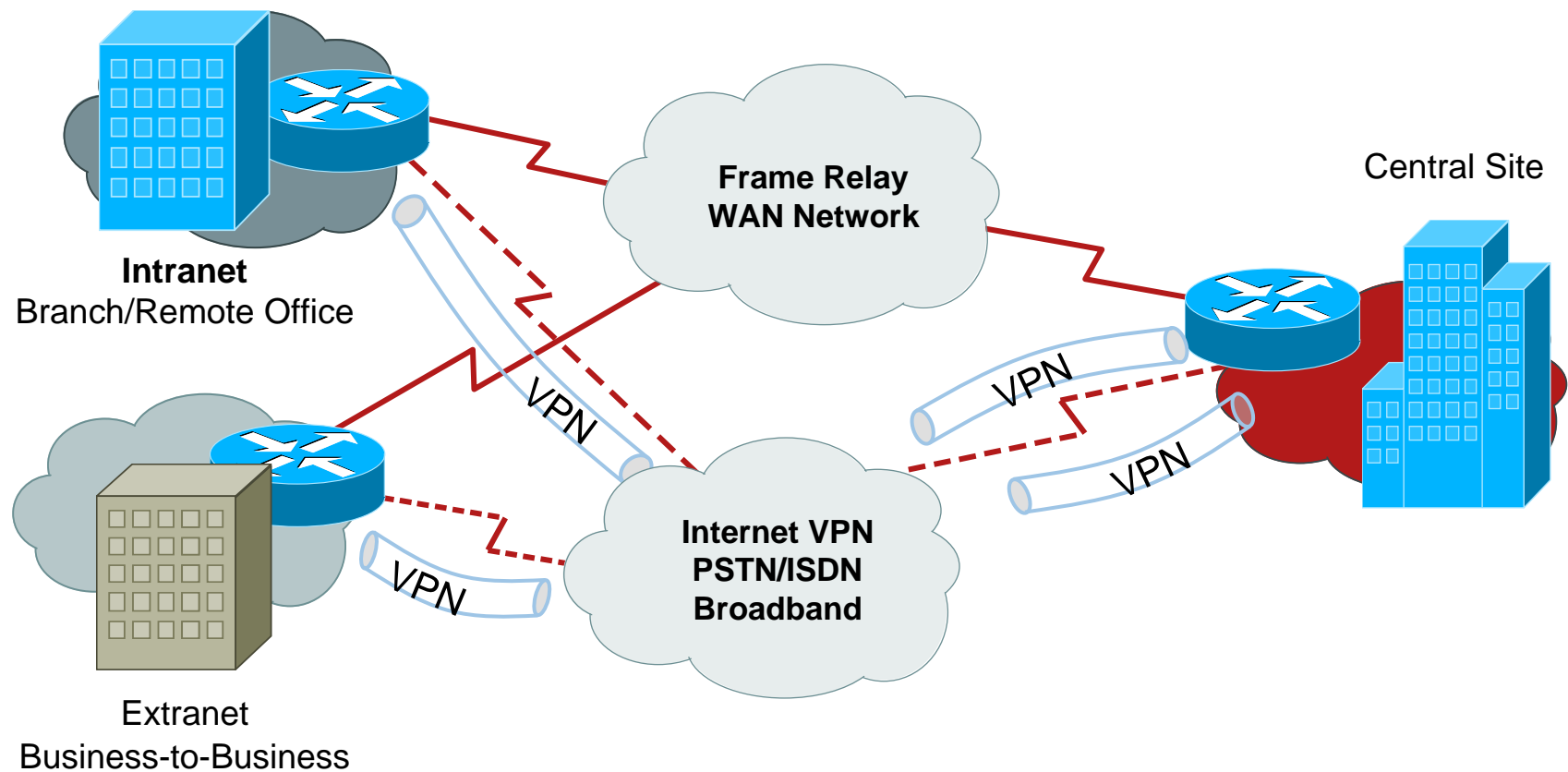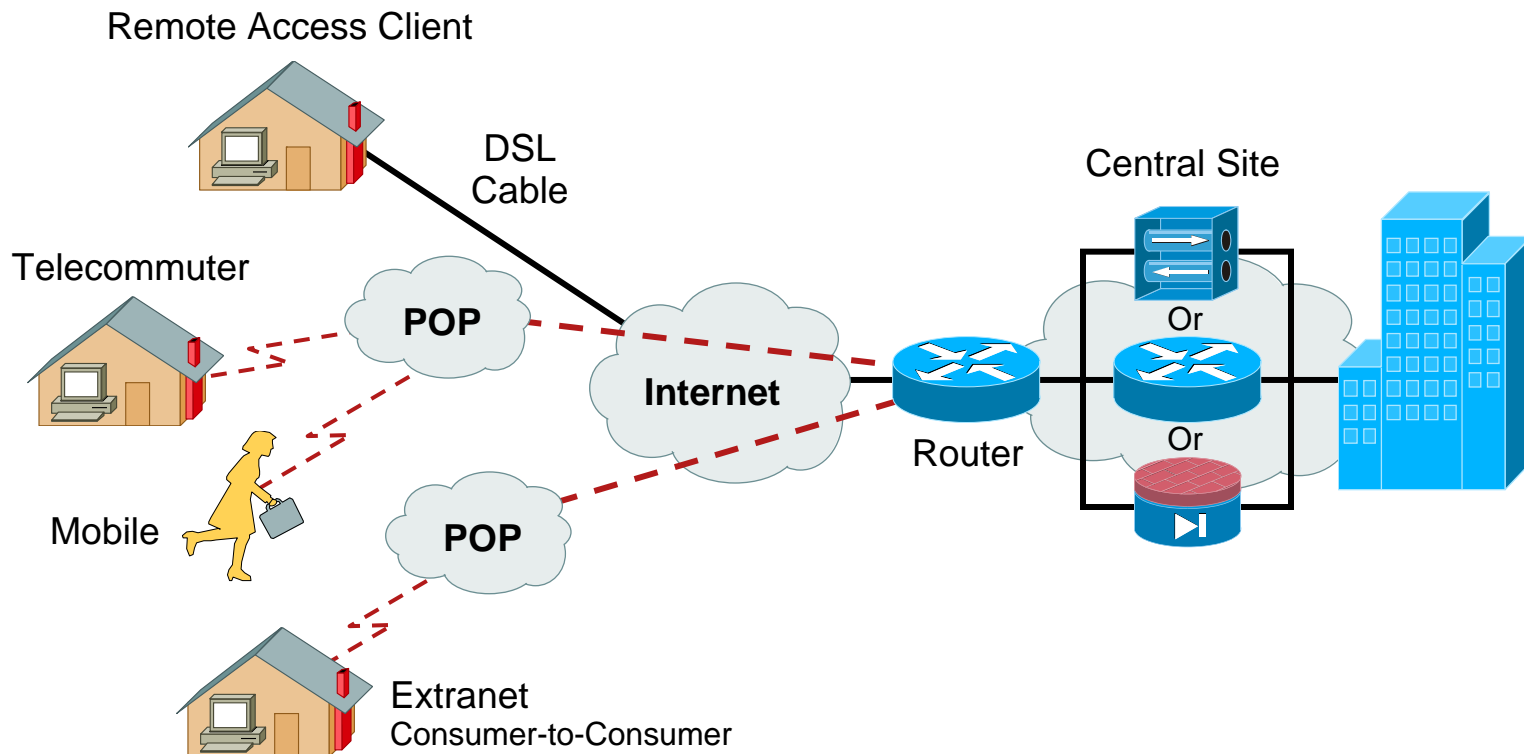(Intranet)

Other Vendors to Router VPN
(Extranet)

Using Site-to-Site VPNs

Intranet
Branch/Remote Office

Frame Relay
WAN Network

Central Site

VPN

Internet VPN
PSTN/ISDN
Broadband

VPN

VPN

VPN

Extranet
Business-to-Business

Using Remote-Access VPNs
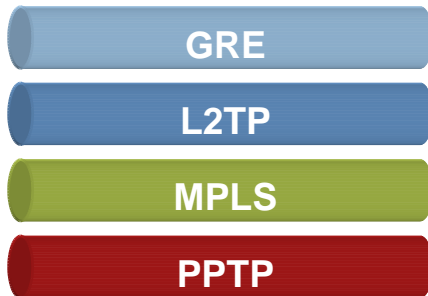

Remote Access Client

- Cisco VPN Clients (IPSec)
- Microsoft Win 9x/NT/2000/XP (LTTPP)
- Thire-party VPN client (PPTP)

Remote Access Gateway

- Cisco WAN Router
- Cisco Secure PIX Firewall
- Or IPSec or PPTP aware device to provide firewall/VPN Tunnel Termination

VPN Components

Separate Data	Increase Protection	Prevent Tampering
Tunneling	**Encryption**	**Integrity**

Separate Data
Tunneling

GRE

L2TP

MPLS

PPTP

Increase Protection
Encryption

IPSec

DES, 3 DES

MPPE

Prevent Tampering
Integrity
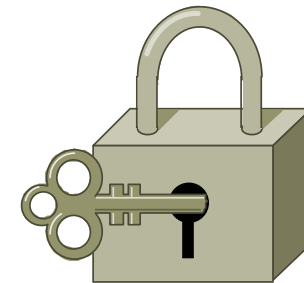
TCP Checksum
AH in IPSec

Identify Source
Authentication

PKI

RSA   RSA

VPN Security

Cisco Public
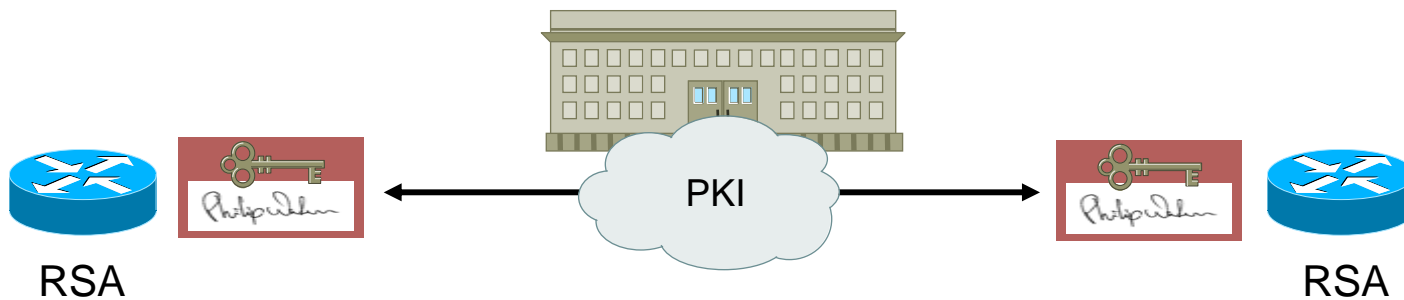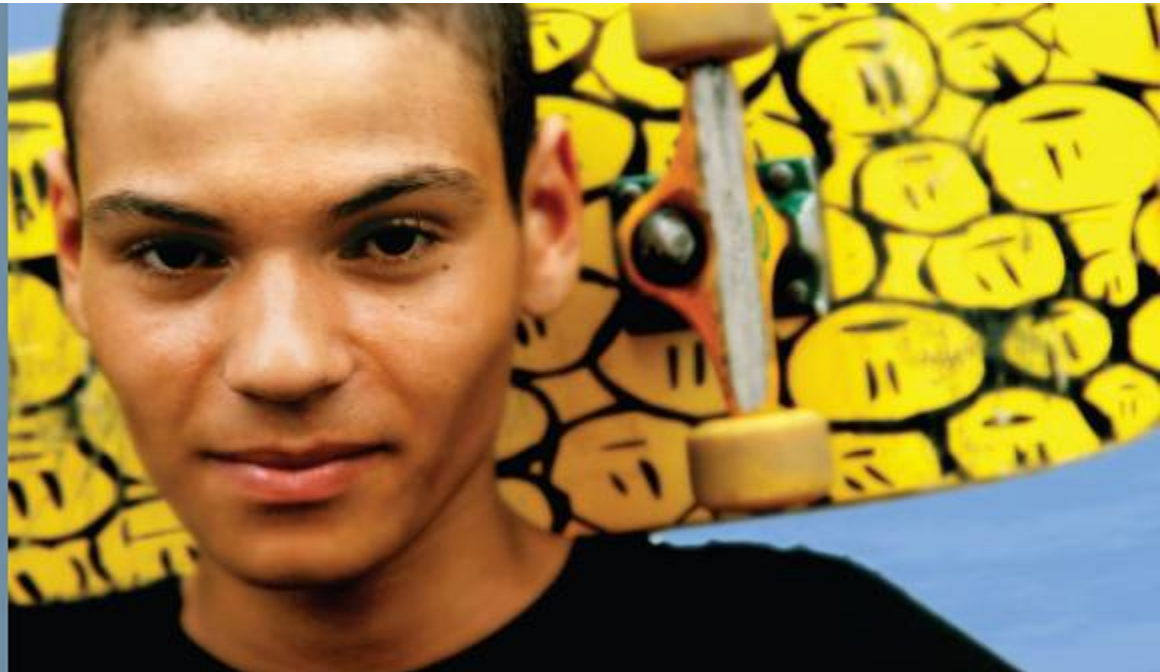
What a VPN Must Provide
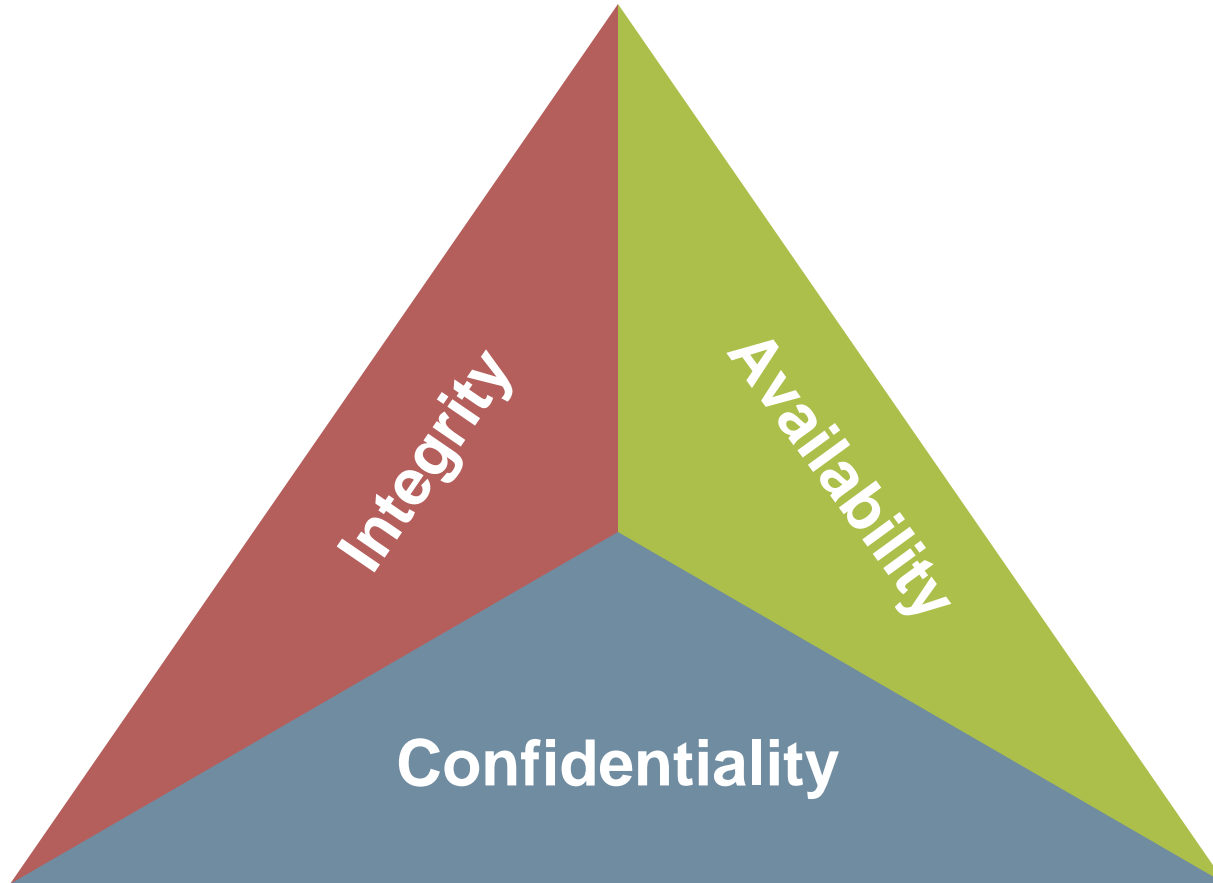
Network Security Model

Data Security Assurance Model (CIA)

Confidentiality

- Benefit
- Ensures data privacy
- Shuns
- Sniffing
- Replay

Integrity

- Benefit

    Ensures data is unaltered during transit

- Shuns

    Alteration

    Replay

Authentication

- Benefit

    Ensures identity of originator or recipient of data

- Shuns

    Impersonation

    Replay

Data Confidentiality and Data Integrity Depend on Encryption and Encapsulation

VPN Technology Options

Application Layer (5–7)

SSH — Application Layer — SSL

Transport/ Network Layer (3–4)

Network Layer

GRE
PPTP
L2TP
MPLS

IPSEC
MPPE

Link/Physical Layer (1–2)

Link-Layer Encryption

Link-Layer Encryption
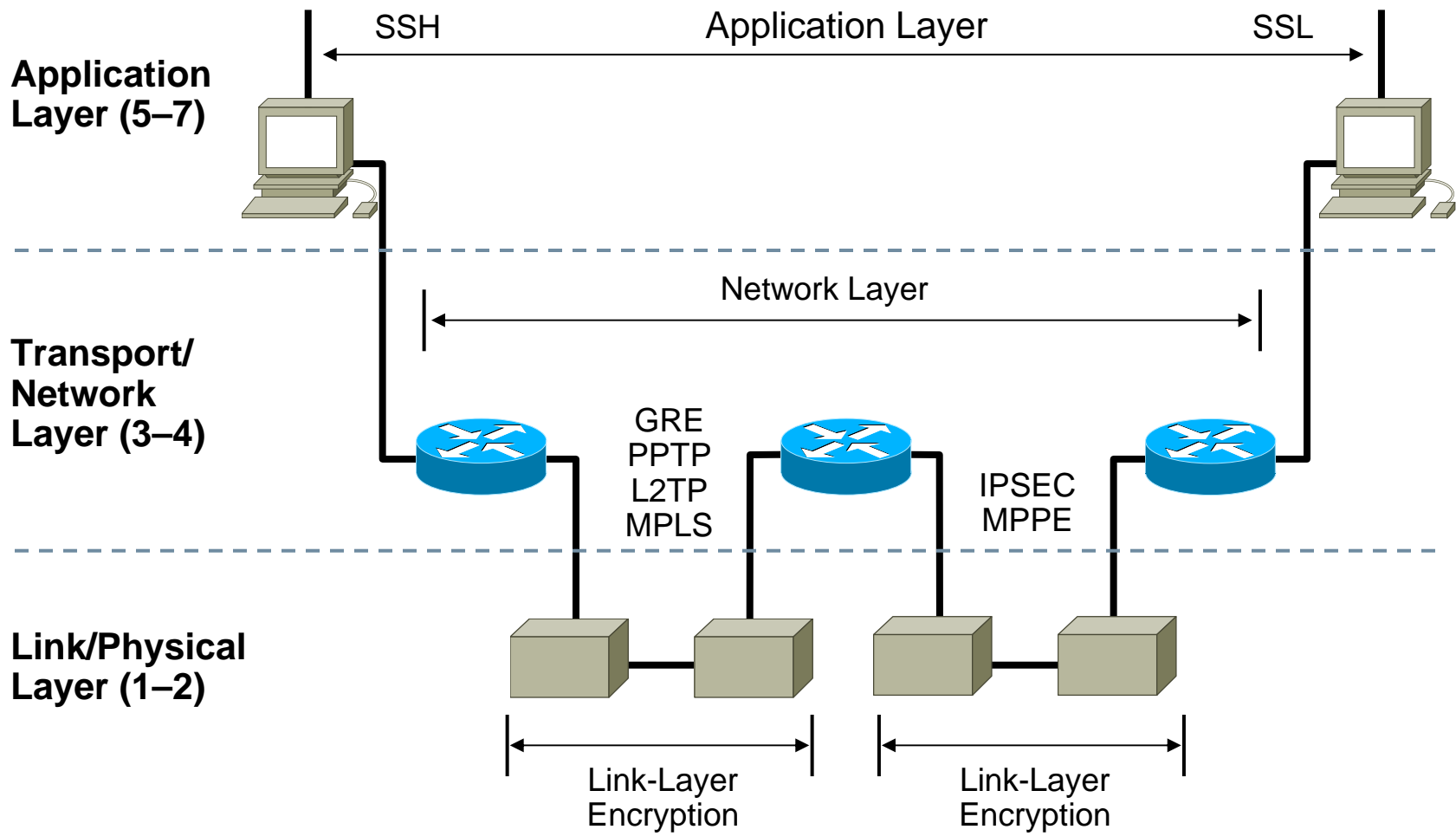
What Is an IPSec VPN?

Internet Protocol Security

- A set of security protocols and algorithms used to secure IP data at the network layer

- IPSec provides data confidentiality (encryption), integrity (hash), authentication (signature/certificates) of IP packets while maintaining the ability to route them through existing IP networks

Advantages of IPSec

- Access VPNs
- Classic site-to-site managed VPNs
- Trusted MPLS VPNs

Service Provider

Main Office

Business Partner

POP

Mobile Worker

Mobile Worker

Remote Office

Regional Office

Home Office

Cisco Public

16
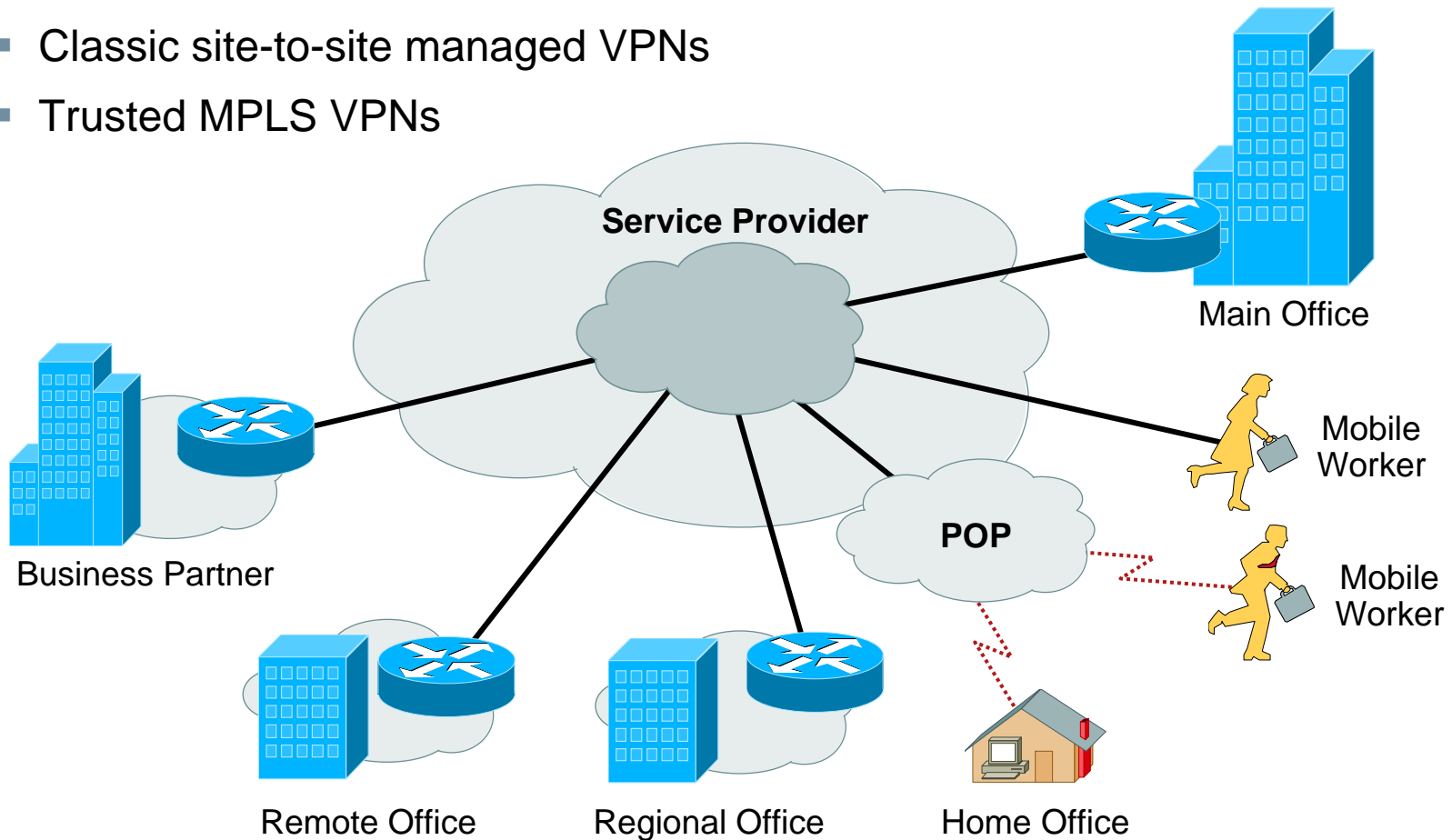
IPSec Key Points

- IPSec can ensure the confidentiality and/or the authenticity of IP packets

- The key points are

  Two modes of propagation (transport and tunnel)

  Security associations (SAs)

  Two types of header (ESP and AH)

IP Data (Encrypted)

ESP Header

AH Header

IP Header

IPSec Framework

IPSec
Framework

Choices

IPSec Protocol

ESP	ESP + AH	AH

Encryption

DES	3 DES	AES

Authentication

MD5	SHA

DH

DH1	DH2	DH5
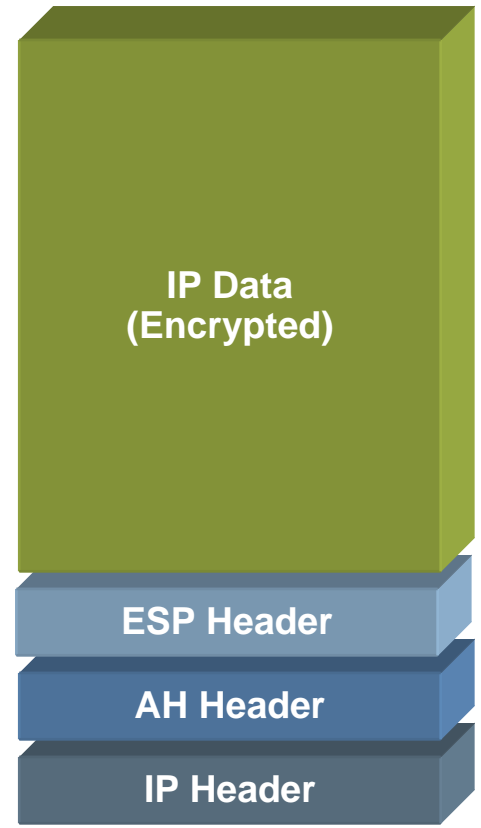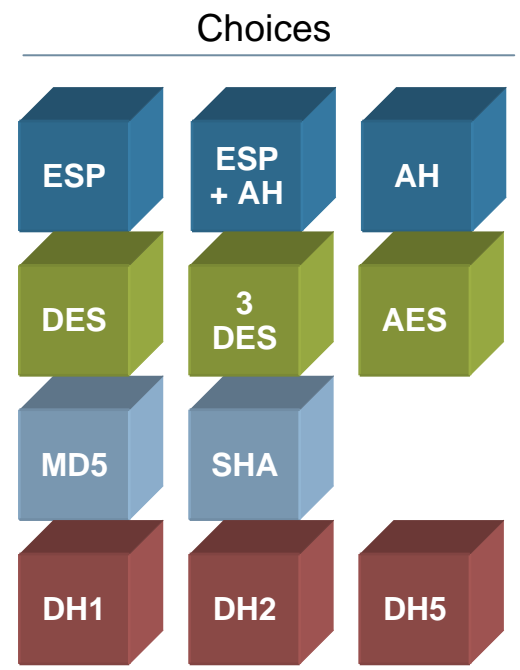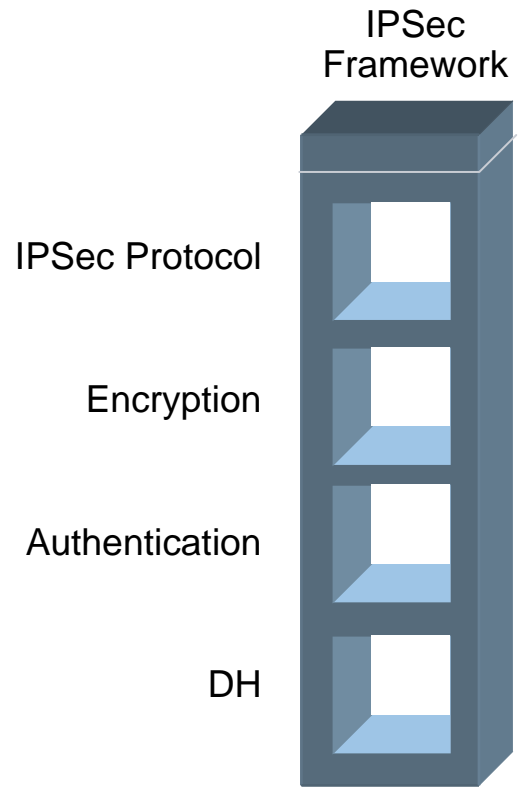
ESP—Encapsulating Security Payload

AH—Authentication Header

AES—Advanced Encryption Standard

MD5, SHA—Authentication

DH—Diffie-Hellman Identifier to Derive the Share Secret

Two Types of IPSec Security Protocols

Authentication Header

All Data in Cleartext

Router A ▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬ Router B

- Ensures data integrity
- Provides origin authentication— ensures packets definitely came from peer router

- Uses keyed-hash mechanism
- Does **not** provide confidentiality (no encryption)
- Provides optional replay protection

Encapsulating Security Payload

Data Payload Is Encrypted

Router A ▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬▬ Router B

- Data confidentiality (encryption)
- Limited traffic flow confidentiality
- Data integrity

- Optional data origin authentication
- Anti-replay protection
- Does not protect IP header

IP Header with IPSec Information

Cisco Public
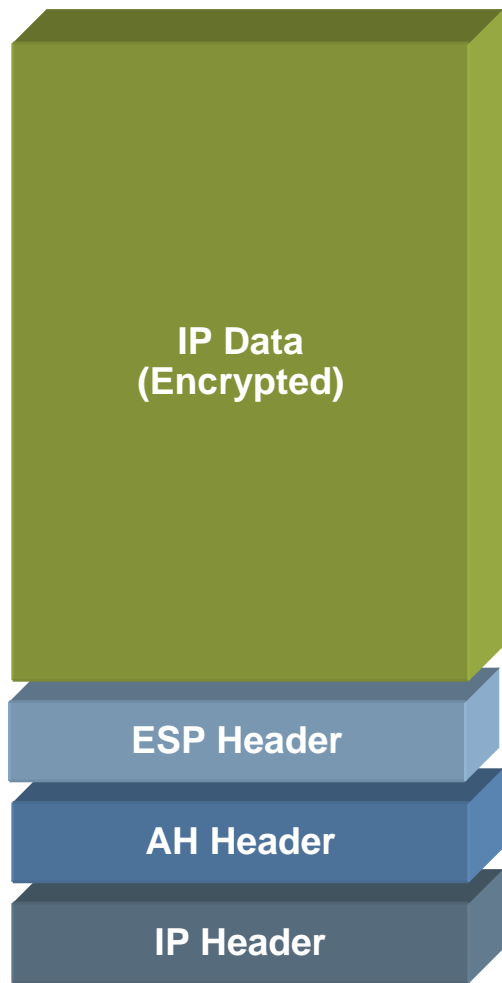
IPSec in a Standards World

Headquarters

Periodic Re-Key

IKE

CERTIFICATE

IPSec

Internet/IP VPN

Router

Firewall

Remote Office

Firewall
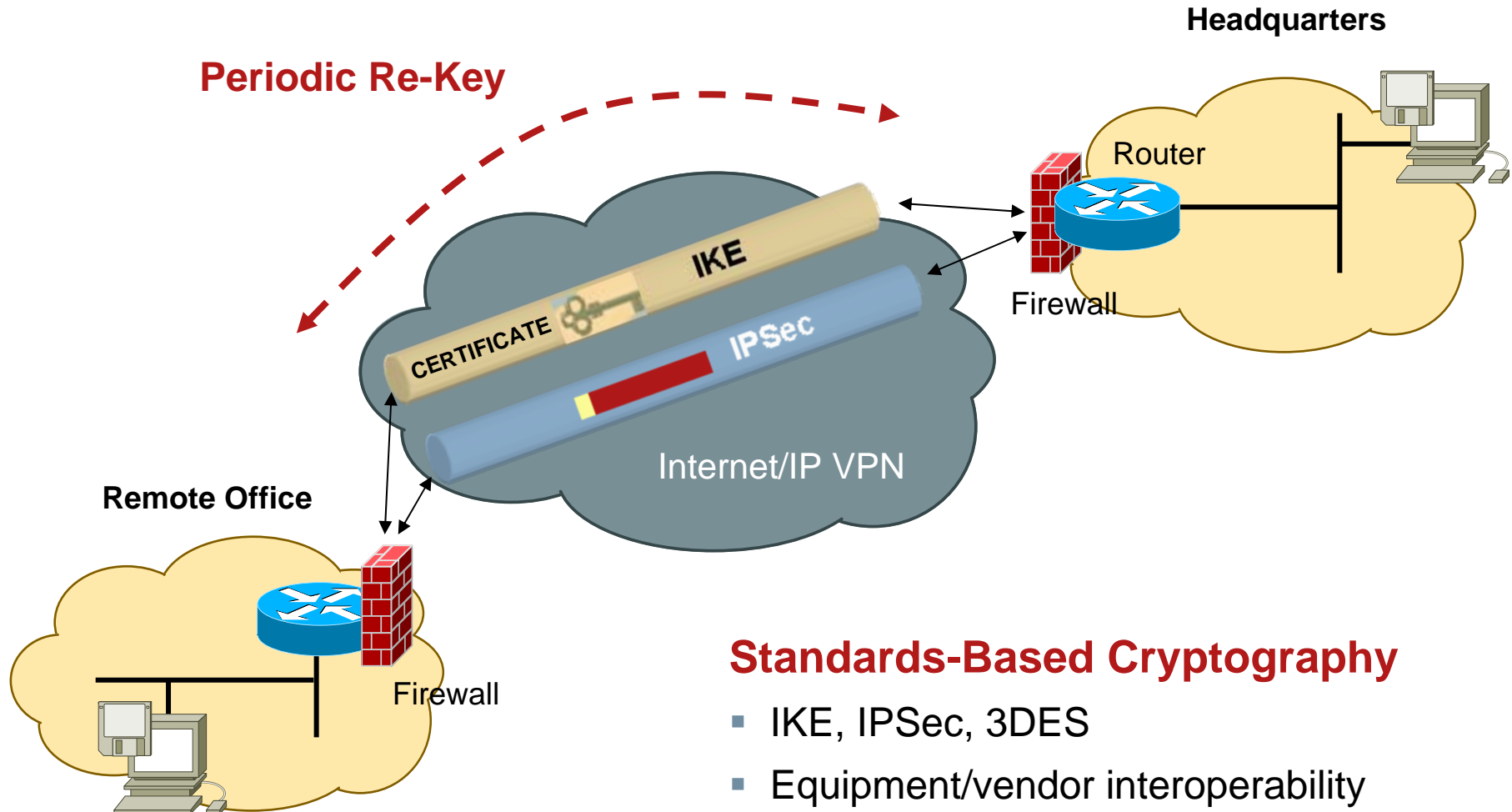
Standards-Based Cryptography

- IKE, IPSec, 3DES
- Equipment/vendor interoperability

IKE Benefits an IPSec Environment

- Ensure confidential communications in an unsecured network
- Also known as the **Key Management Nightmare!!!**

IPSec: Building a Connection

IKE (Phase 1)

IKE (Phase 2)
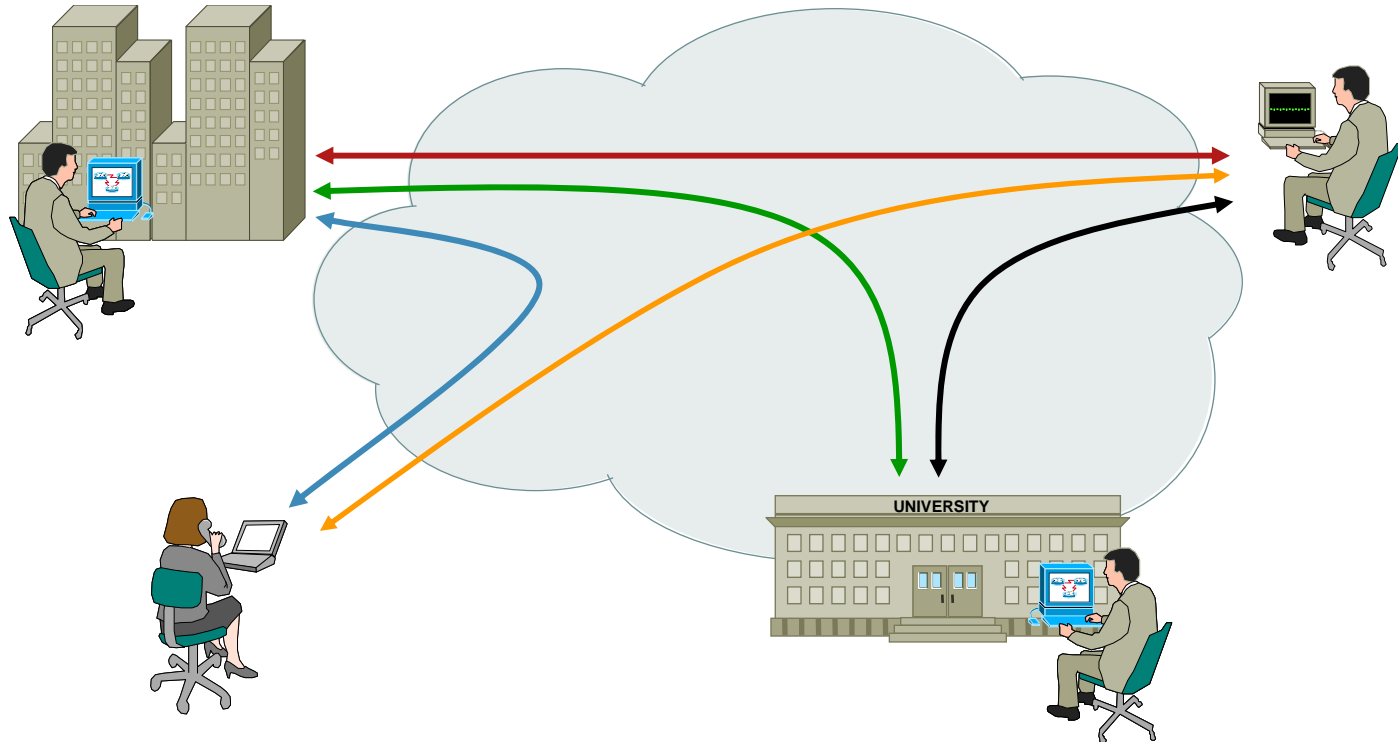
Data
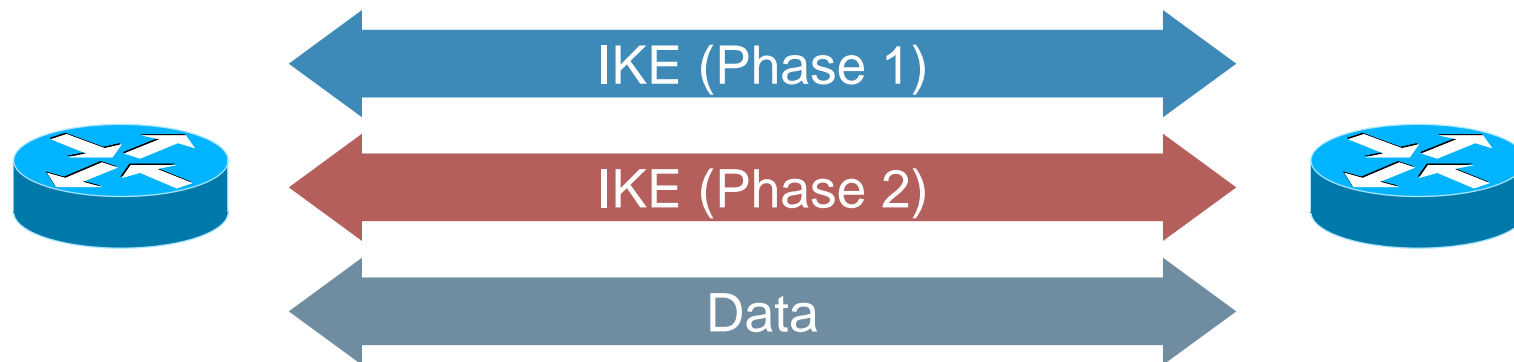
- Two-phase protocol:

    Phase 1 exchange: two peers establish a secure, authenticated channel with which to communicate; Main mode or Aggressive mode accomplishes a Phase 1 exchange

    Phase 2 exchange: security associations are negotiated on behalf of IPSec services; Quick mode accomplishes a Phase 2 exchange

- Each phase has its SAs: ISAKMP SA (Phase 1) and IPSec SA (Phase 2)

How Does IKE/IPSec Work?

Phase I SA (ISAKMP SA)

| Main Mode (6 Messages) | Aggressive Mode (3 Messages) |

New IPSec Tunnel or Rekey

Phase II SA (IPSec SA)

Quick Mode

....

Phase II SA (IPSec SA)

Quick Mode

A Protected Data B

C Protected Data D
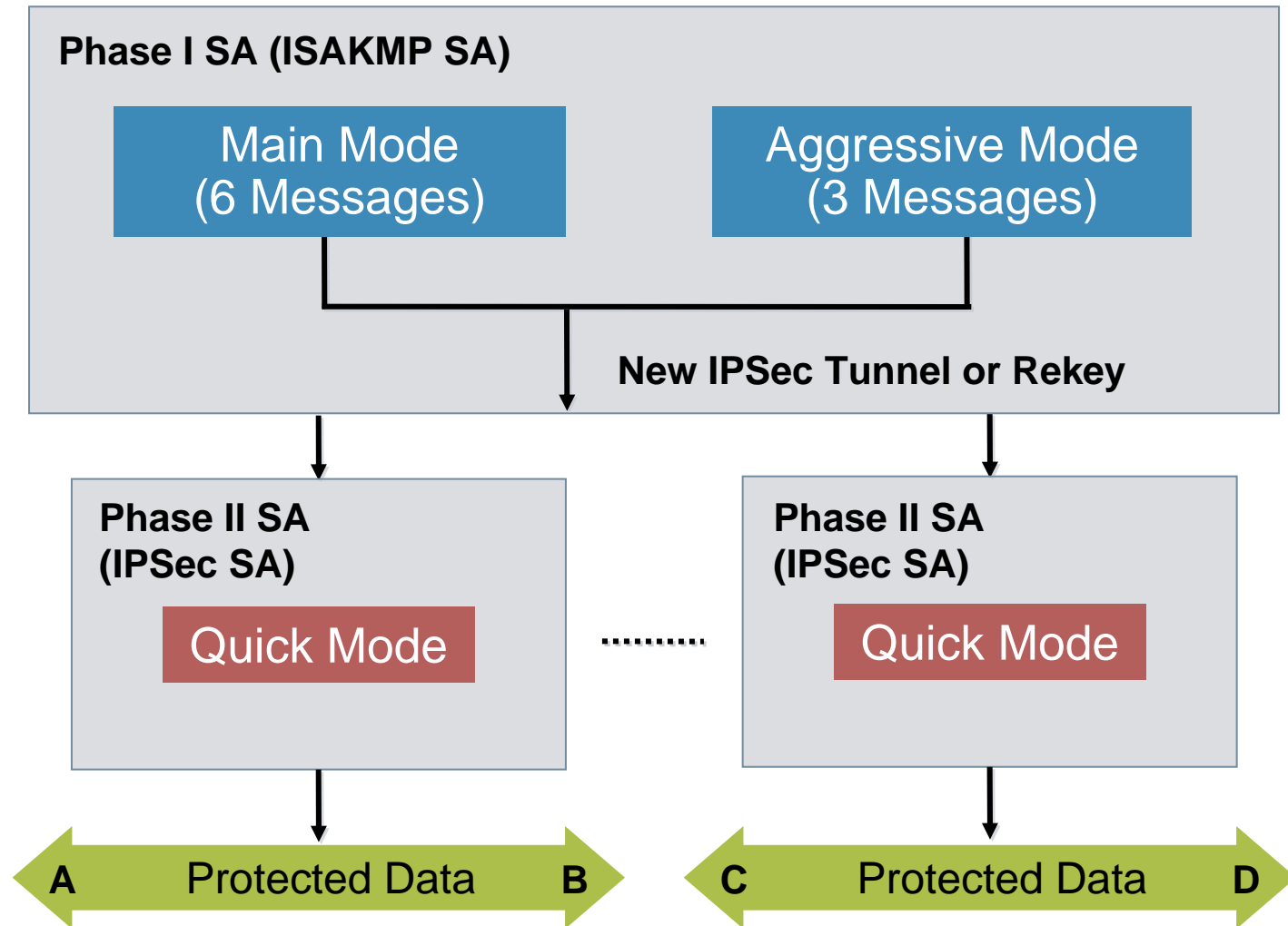
ISAKMP Main, Quick and Aggressive Modes

ISAKMP Main Mode (Phase 1)

INITIATOR

SA	Header	**1** →
← **2**	Header	SA
Nonce	Key	Header	**3** →
← **4**	Header	Key	Nonce
Sig	[Cert]	ID	Header	**5** →
← **6**	Header	ID	[Cert]	Sig

RESPONDER
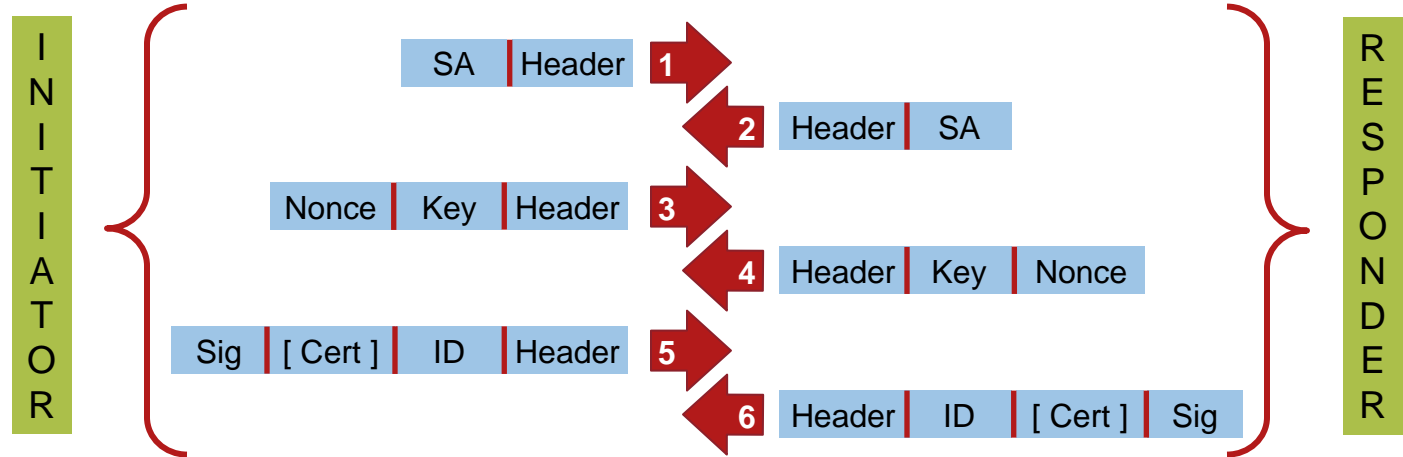
ISAKMP Quick Mode (Phase 2)

ID/ID	[Key]	Nonce	SA	Hash	Header	**1** →
← **2**	Header	Hash	SA	Nonce	[Key]	ID /ID
Hash	Header	**3** →
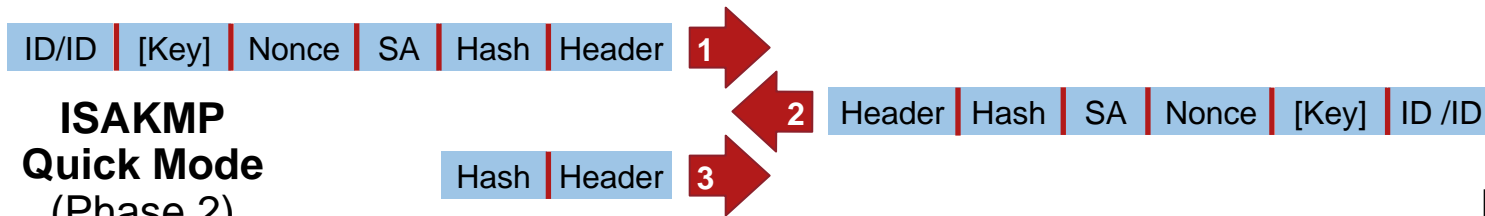
ISAKMP Aggressive Mode (Phase 1)

ID	Nonce	[Key]	SA	Header	**1** →
← **2**	Header	SA	[Key]	Nonce	ID	[Cert]	Sig
Sig	[Cert]	Header	**3** →

What Is a Web/SSL VPN?
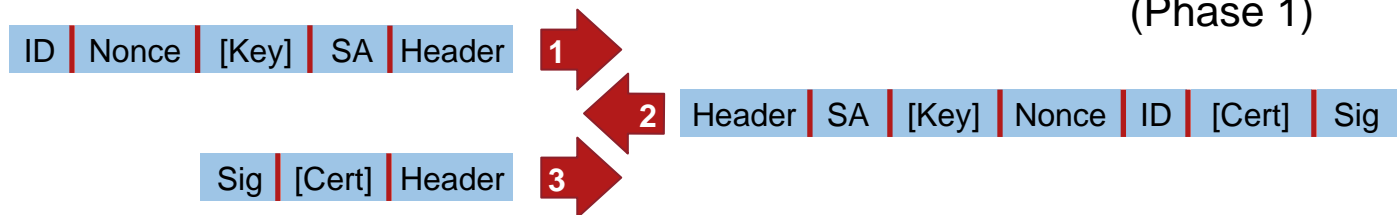
Certificate
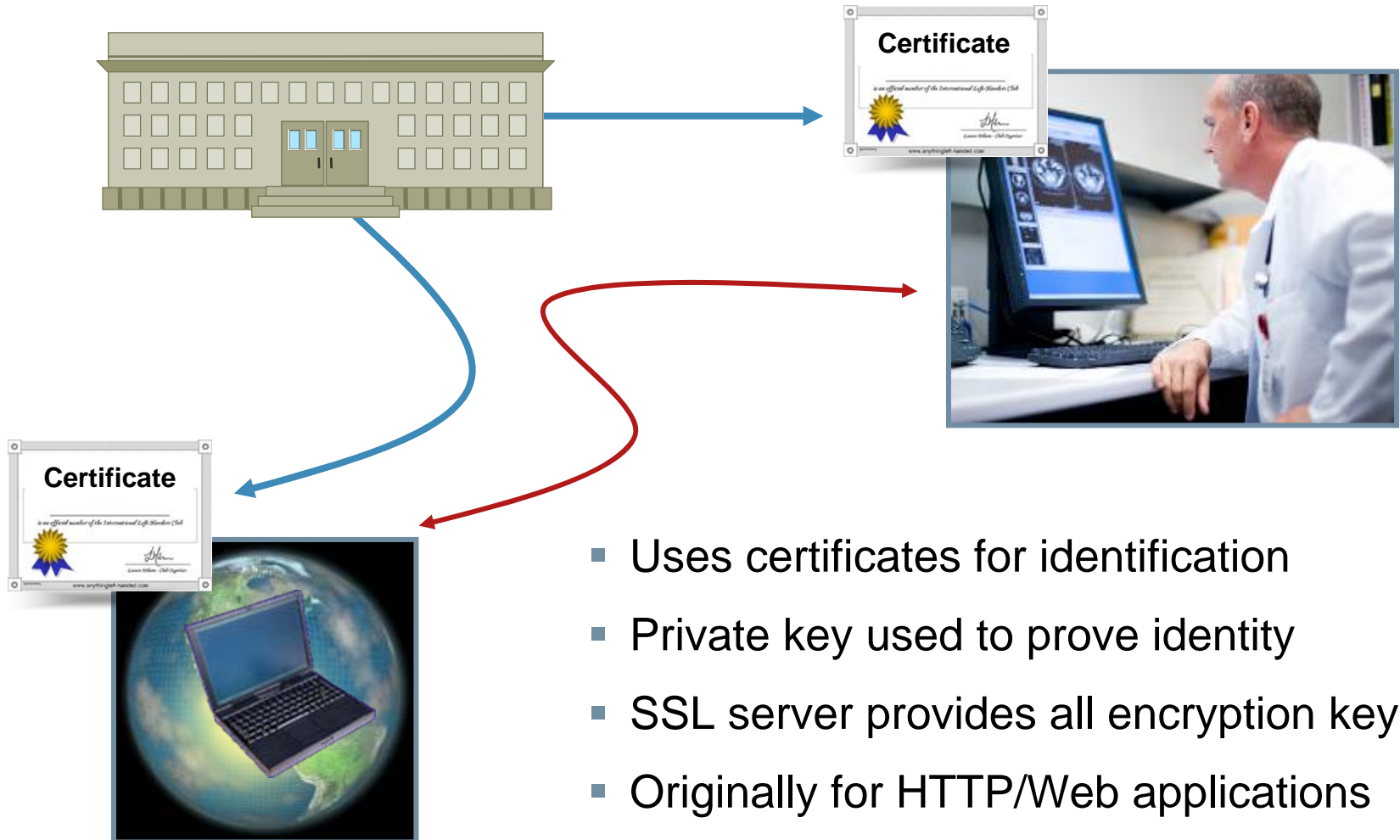
Certificate

- Uses certificates for identification
- Private key used to prove identity
- SSL server provides all encryption keys
- Originally for HTTP/Web applications

Web/SSL VPN Features

WebVPN

Broadband Modem

Broadband Provider

ISP

Encrypted Tunnel

Corporate Network

ASA Firewall

WebVPN

Access Point

Encrypted Tunnel

Wireless LAN
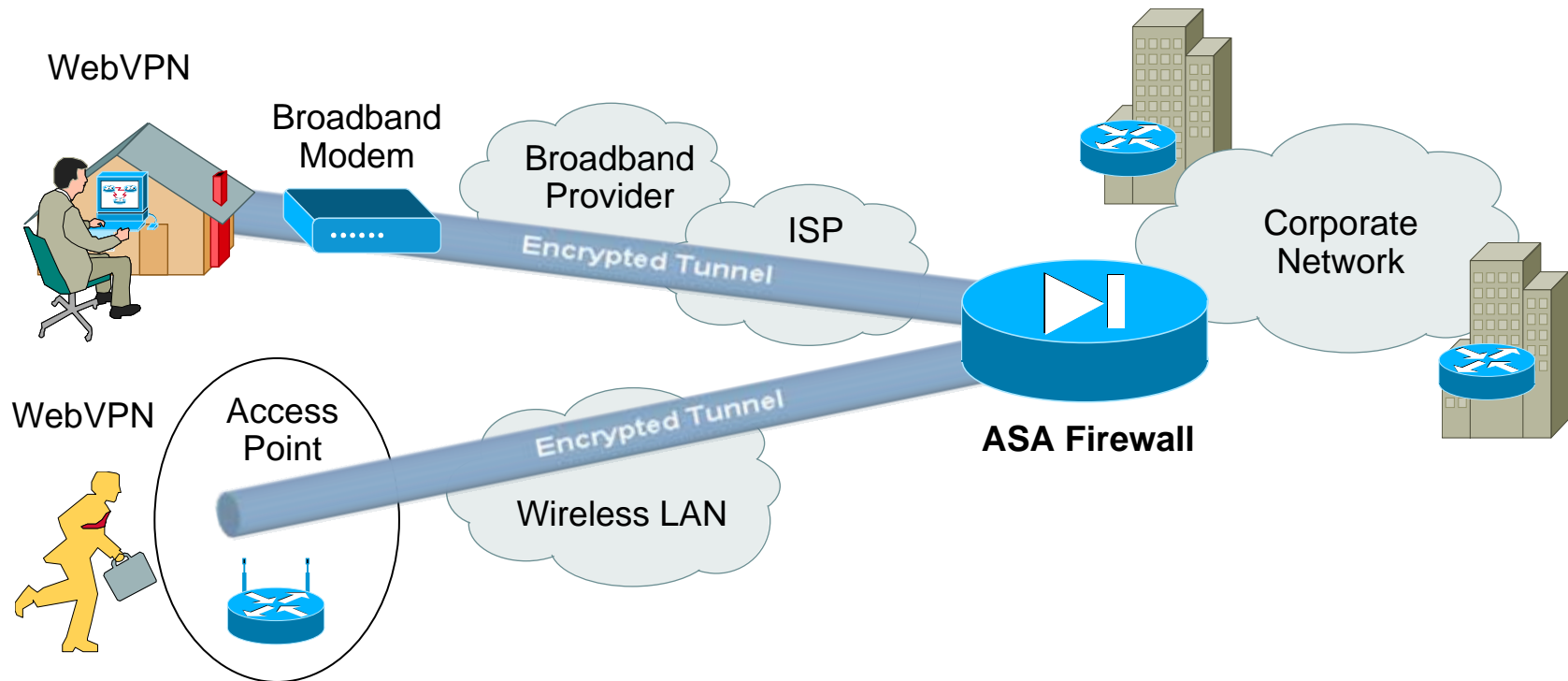
Feature

- Access to internal web sites (HTTP/HTTPS) including filtering
- Access to internal Windows (CIFS) File Shares
- TCP port forwarding for legacy application support
- Access to e-mail via POP, SMTP, and IMAP4 over SSL

Web/SSL VPN and IPSec Comparison

WebVPN

- Uses a standard web browser to access the corporate network

- SSL encryption native to browser provides transport security

- Application accessed through browser portal

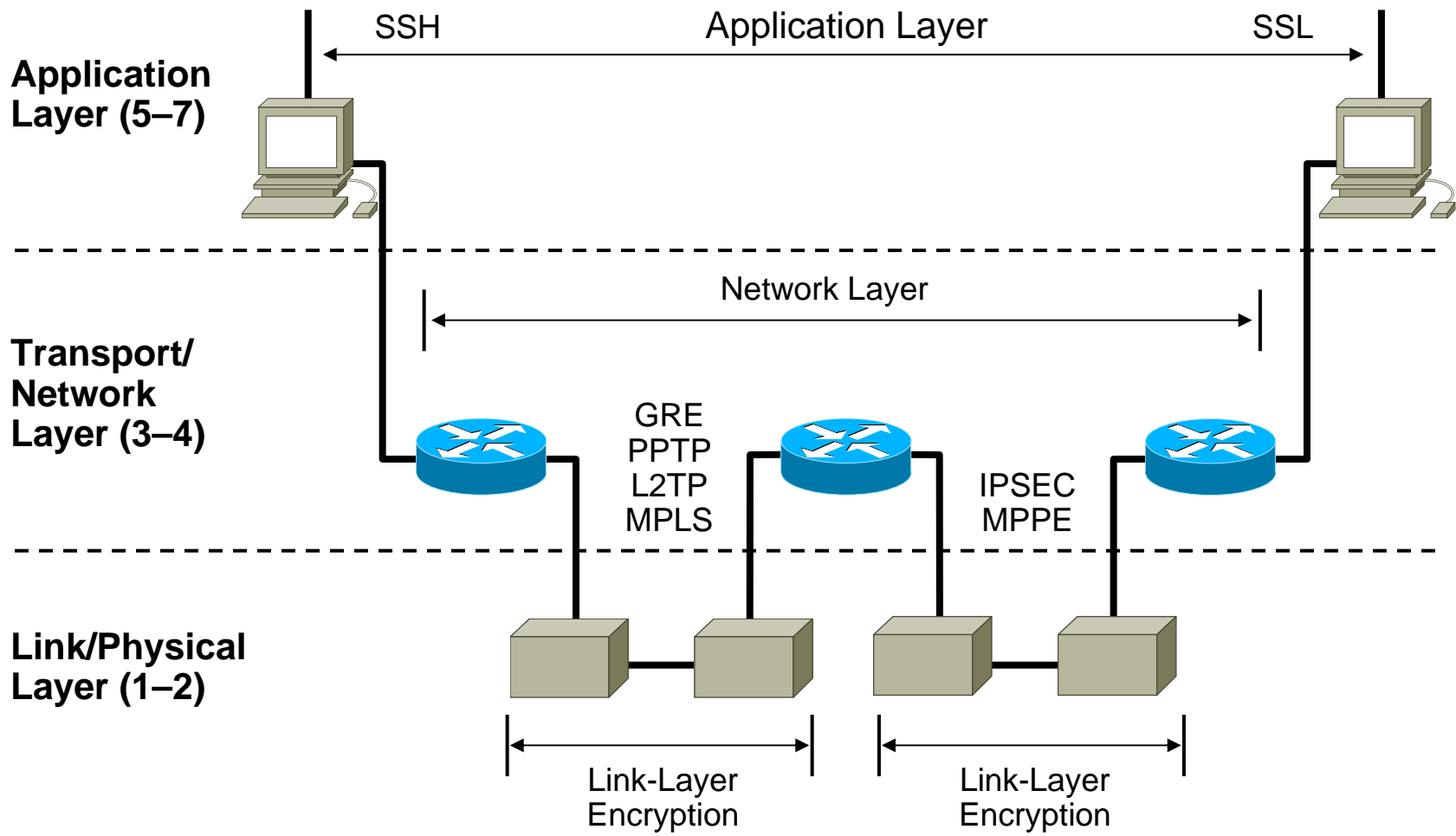- Limited client/server application accessed using applets

IPSEC VPN

- Uses purpose built client software for network access

- Client provides encryption and desktop security

- Client establishes seamless connection to network

- All application are accessible through their native interface

What Is a PPTP VPN?

Point to Point Tunneling Protocol

- PPTP is a network protocol used in the implementation of Virtual Private Networks (VPN); RFC 2637 is the PPTP technical specification

- PPTP works on a client server model; PPTP clients are included by default in Microsoft Windows and also available for both Linux and Mac OS X; newer VPN technologies like L2TP and IPSec may replace PPTP someday, but PPTP/MPPE remains a popular network protocol especially on Windows computers

VPN Technology Options

SSH Application Layer SSL

Application Layer (5–7)

Network Layer

Transport/ Network Layer (3–4)

GRE
PPTP
L2TP
MPLS

IPSEC
MPPE

Link/Physical Layer (1–2)

Link-Layer Encryption

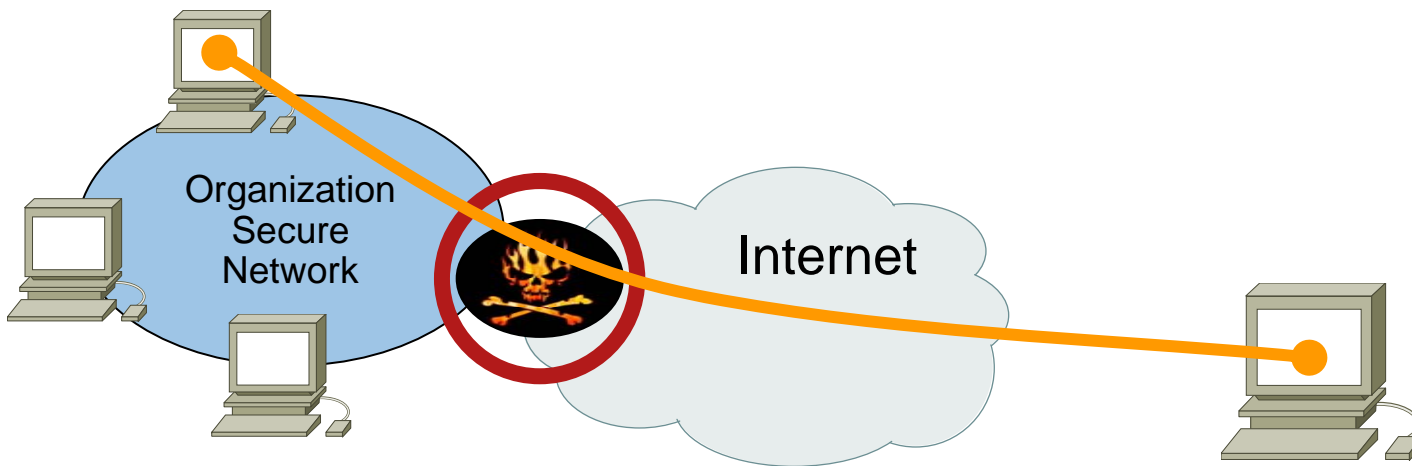Link-Layer Encryption

Benefits of PPTP

					User Data
				TCP	User Data
			IP	TCP	User Data
		PPP	IP	TCP	User Data

GRE	PPP	IP	TCP	User Data
IP	GRE	PPP	IP	TCP	User Data
PPP	IP	GRE	PPP	IP	TCP	User Data

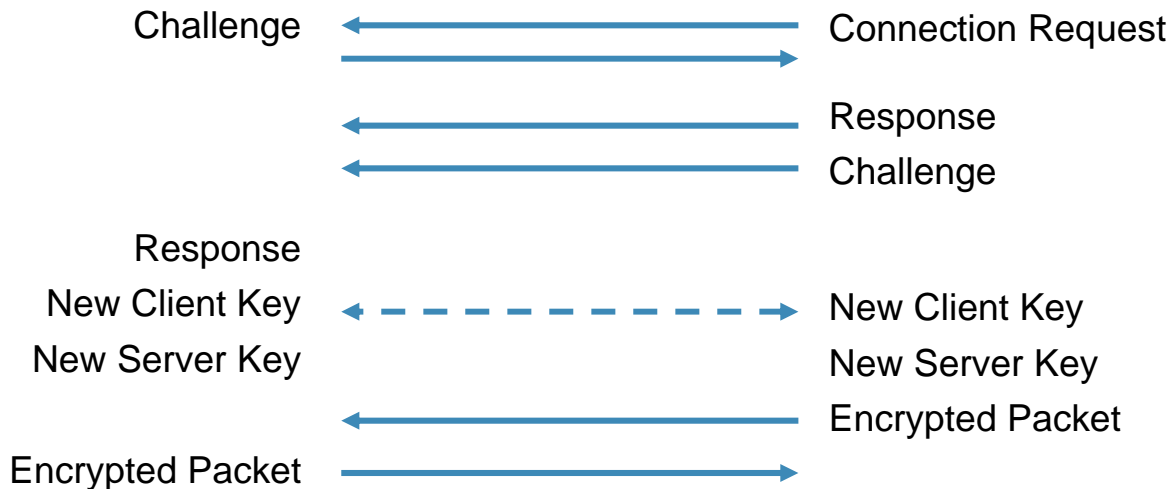Organization Secure Network

Internet
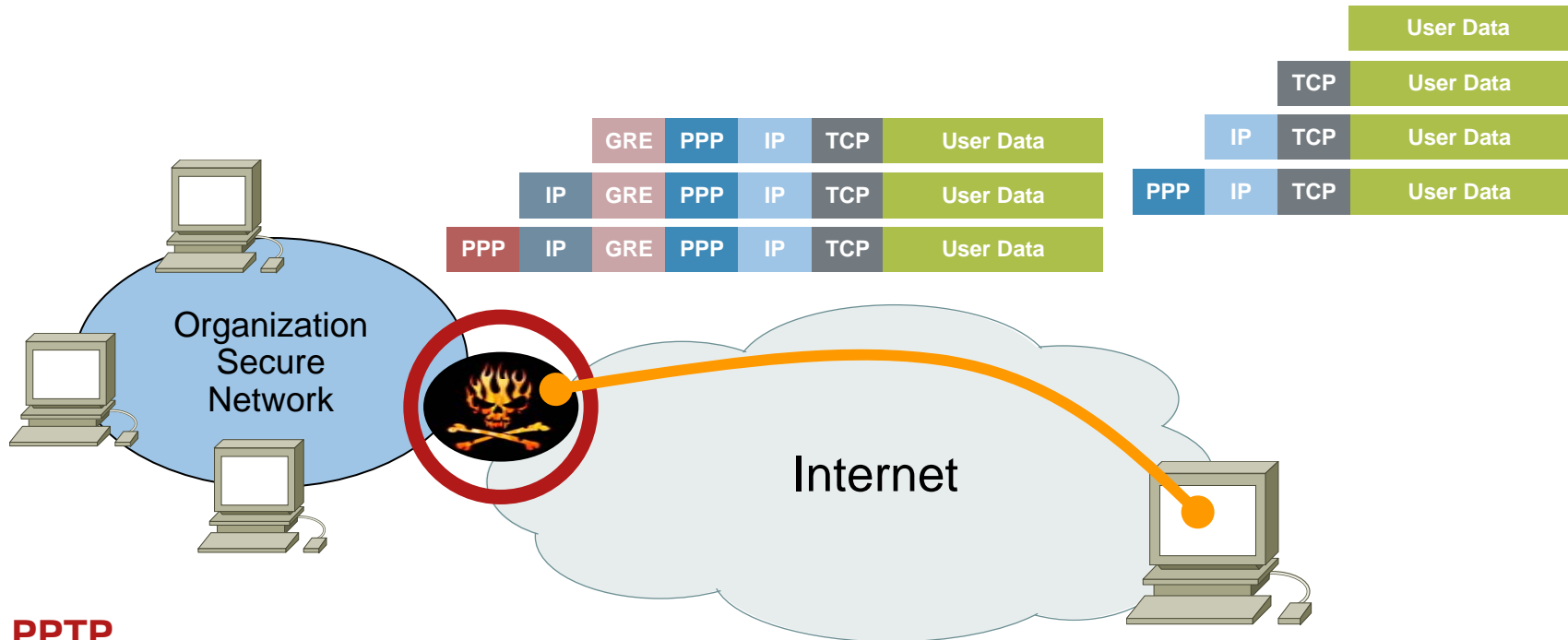
PPTP

- PPoE is point-point protocol over Ethernet
- Single tunnel between end-points: Single device support (GRE = generic routing encapsulation)
- Six bytes over overhead when compression used
- No tunnel authentication
- With RADIUS server supports authentication and accounting
- CHAP V2 fixes password, masquerading, and encryption weakness
- 40 or 128 bit RC4 packet encryption

Is PPTP Secure? Yes

CHAP V2 Authentication with 40 or 128 bit RC4 Encryption

Challenge	← →	Connection Request
	←	Response
	←	Challenge
Response		
New Client Key	← -- →	New Client Key
New Server Key		New Server Key
	←	Encrypted Packet
Encrypted Packet	→	

Cisco Public

VPN Technology Comparison

	Simplicity Low Cost		Advanced Security
Application to Application	SSL		
End to End	IPSec Transport Mode		
Gateway to Gateway	PPTP		L2TP/IPSec IPSec Tunnel Mode
Client to Gateway	PPTP		L2TP/IPSec

PPTP—Point to Point Tunneling Protocol—Layer 2—Multiprotocol
L2TP/IPSec—Layer 2 Tunneling Protocol—Multiprotocol—Encryption and Authentication
IPSec—IP Security—Layer 3—IP Protocol—Encryption and Authentication
SSL—Secure Sockets Layer—Layer 6/7—Application—Encryption and Authentication

Group Exercise
Configuring
VPNs Lab

Cisco Public

Summary

- Demonstration

- Introduction to VPNs

- VPN Security (IPSec, PPTP, SSL)

- VPN Technology Comparison

- VPN Group Exercise